



ETSI/IQC Quantum Safe Cryptography
Conference 2026

Deploying Quantum-Safe Connectivity at Scale: Lessons from a NaaS-Based Approach

Presented by: Antonella Sanguineti



18/06/2026

© ETSI 2026. All rights reserved.

SPARKLE GLOBAL BACKBONE

600.000

Km of fiber

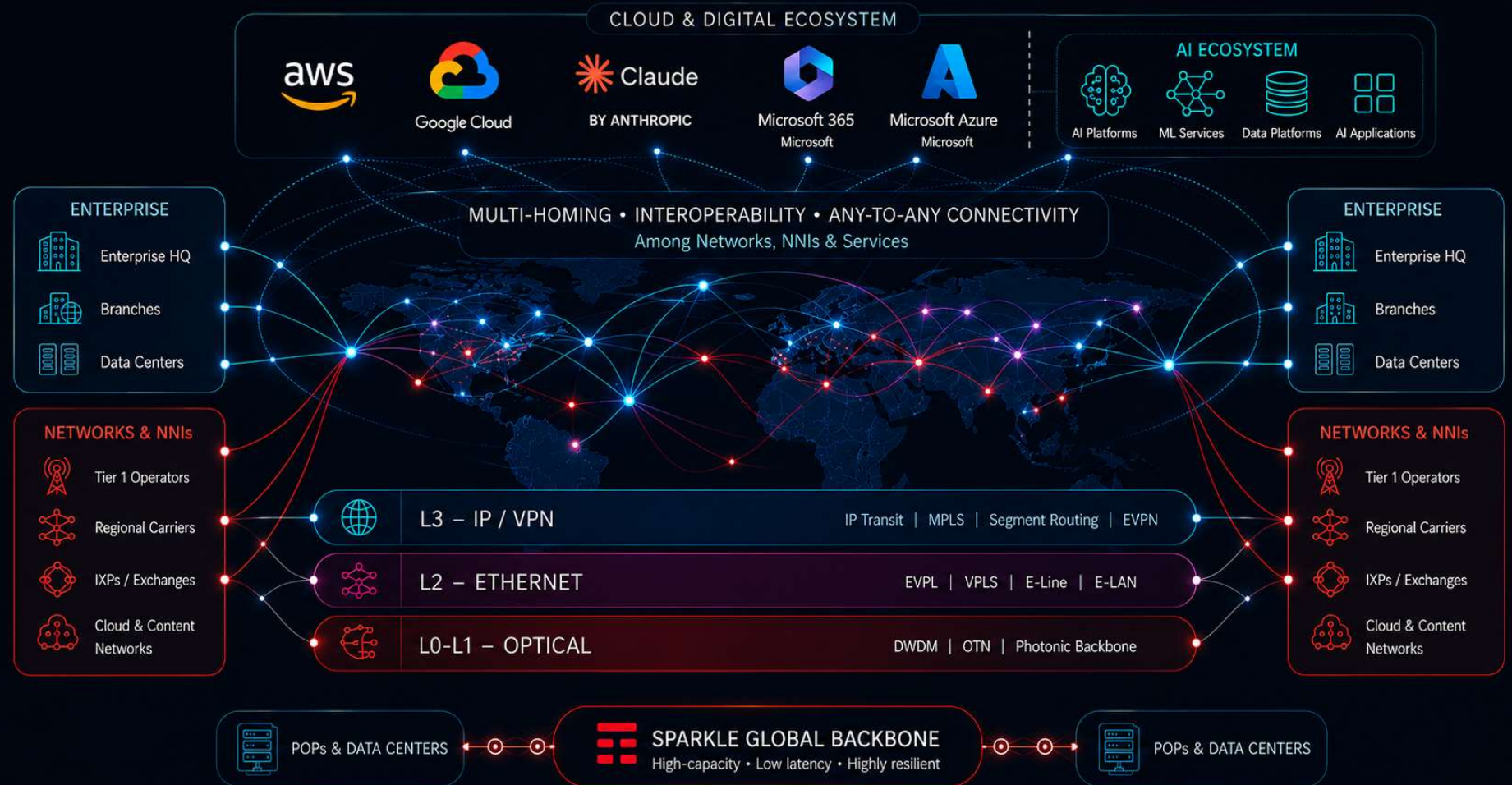
$(X+Y) > Z$

Mosca theorem

9093

Connections

Sparkle multi-layer network



Our requirements



End-to-end

- Smooth interoperability
- Legacy networks



Scalability

- Thousands of endpoints Bandwidth Customer premise
– 10Mb-400Gb



Portability

- DC
- Cloud
- Exchanges



Performance & Certifications

- No compromise
- Compliance



Agility

- Flexible deployment
- Easy update
- Technology agnostic



Time

- Adoption & Integration



Cost

- Security as investment, but a budget issue



Observability

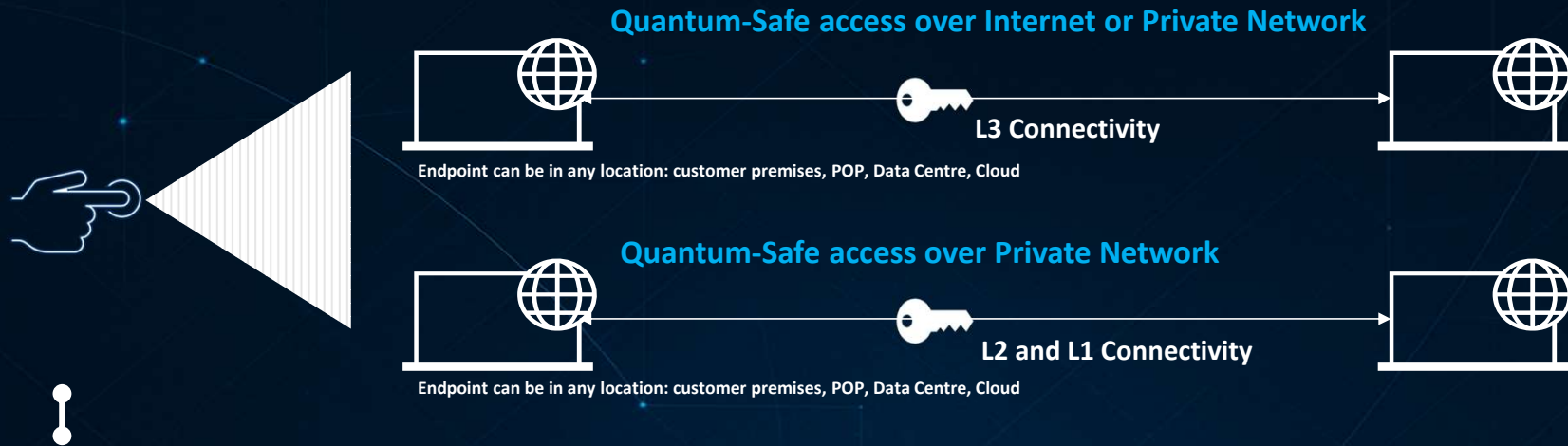
- One platform, many network layers
- APIs for easy integration

Sparkle Network as a Service (NaaS)



Network functionalities On-Demand, Cybersecurity, AI, Cloud-based orchestration and automation

Network as a Service QSI - Concept



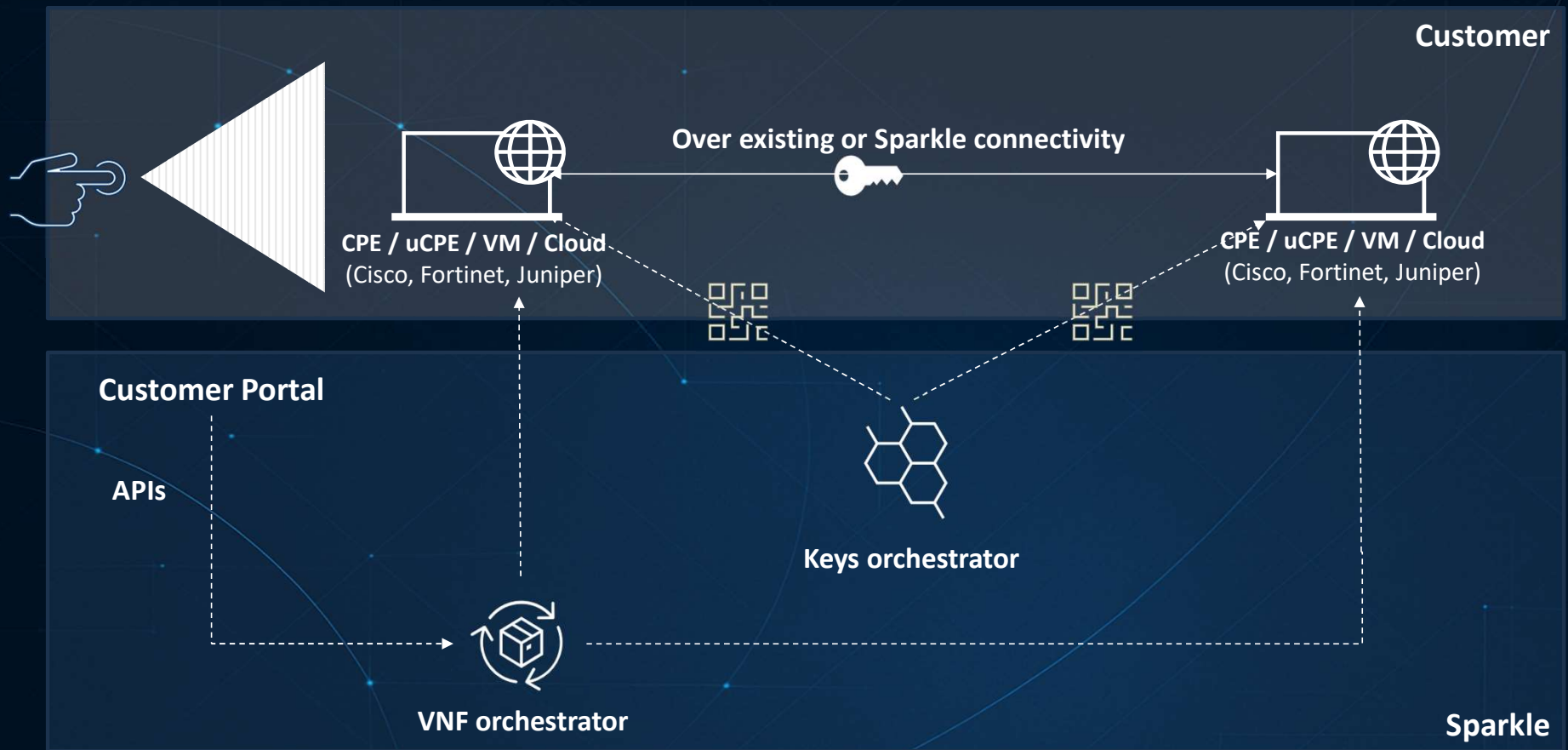
On-demand set-up

- On-demand VPN and Internet Access
- On-demand Post Quantum turn-on/off
- Monitoring on Customer Portal
- Sparkle NOC/SOC for managed solution

Symmetric Key Agreement

- Keys can be used to secure any channels (IPsec, MACsec, TLS, MQTT)
- **Continuous** keys rotation
- **Centralized** key management
- **Crypto-agile** as the underlying cryptographic primitives can be upgraded or replaced

Network as a Service QSI - Components



Network as a Service QSI– High Level Solution

NaaS Services Platform

Sparkle Customer Portal

SPARKLE Home NaaS Cases Network Events Orders Assets More

Product Catalog

- Quantum Safe over Internet
- IP VPN
- Internet Access
- Cloud Connect
- Ethernet

VNFs Orchestrator

Deployment Status of VNFs

Activity

Service Status: Fully Operational

Total Devices: 14

Total Users: 8

Recent Activity

Auto Refresh

Symmetric Key Agreement

ARCIT NaaS Platform

Activity

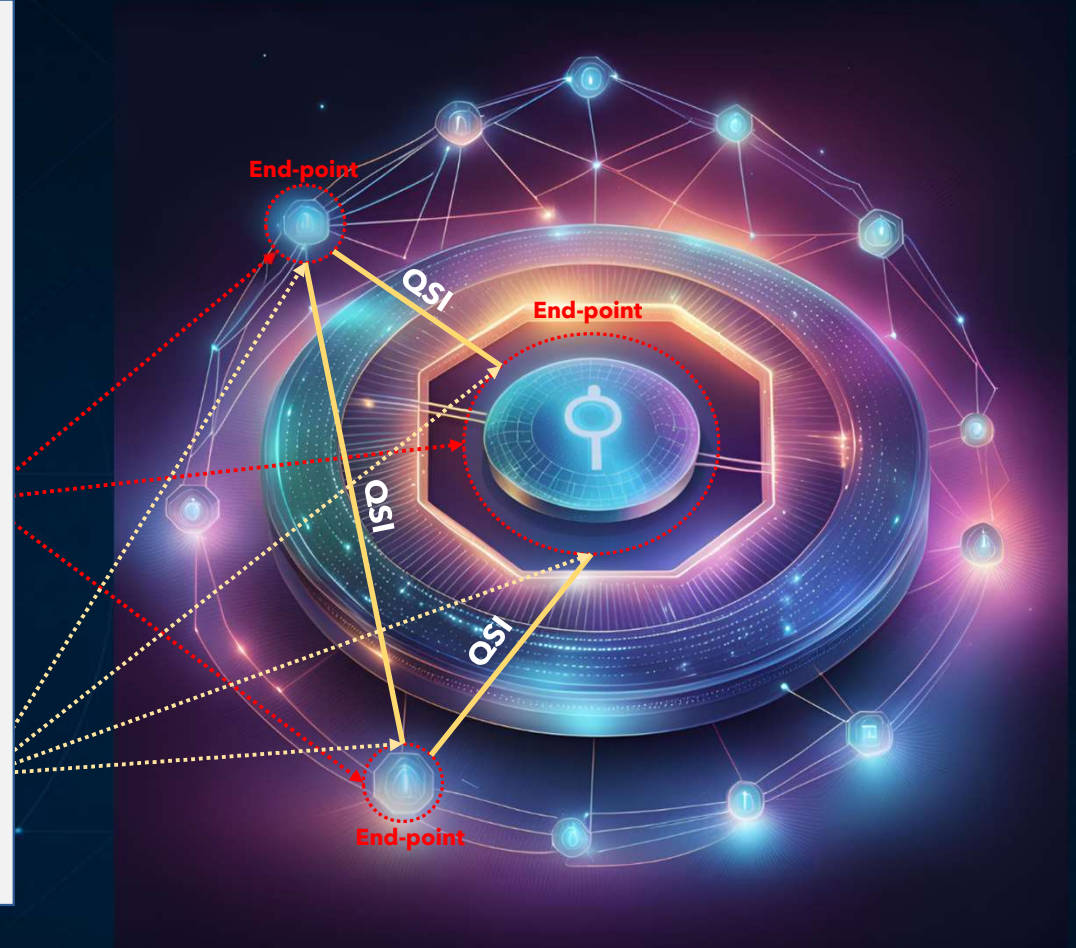
Service Status: Fully Operational

Total Devices: 14

Total Users: 8

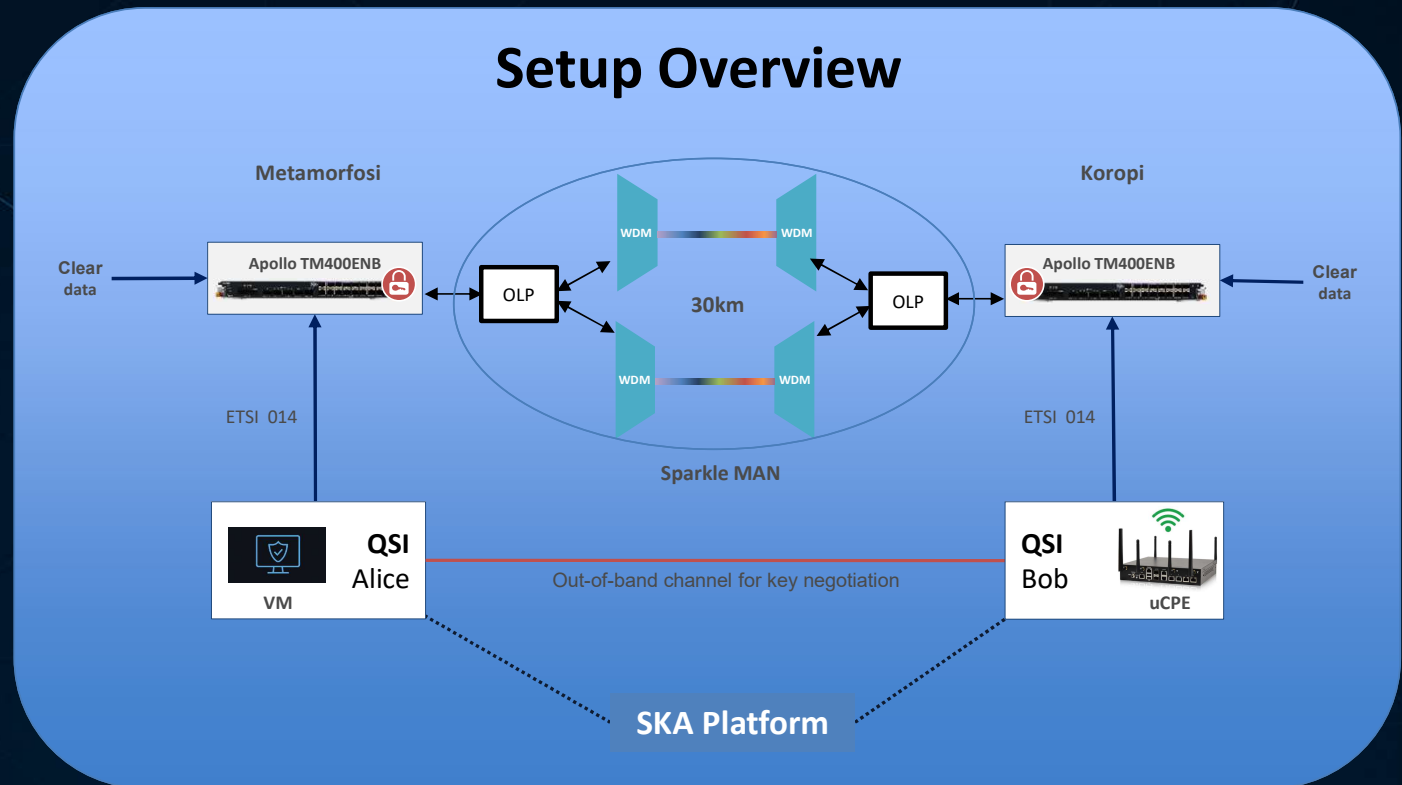
Recent Activity

Auto Refresh



Quantum Safe over Optical

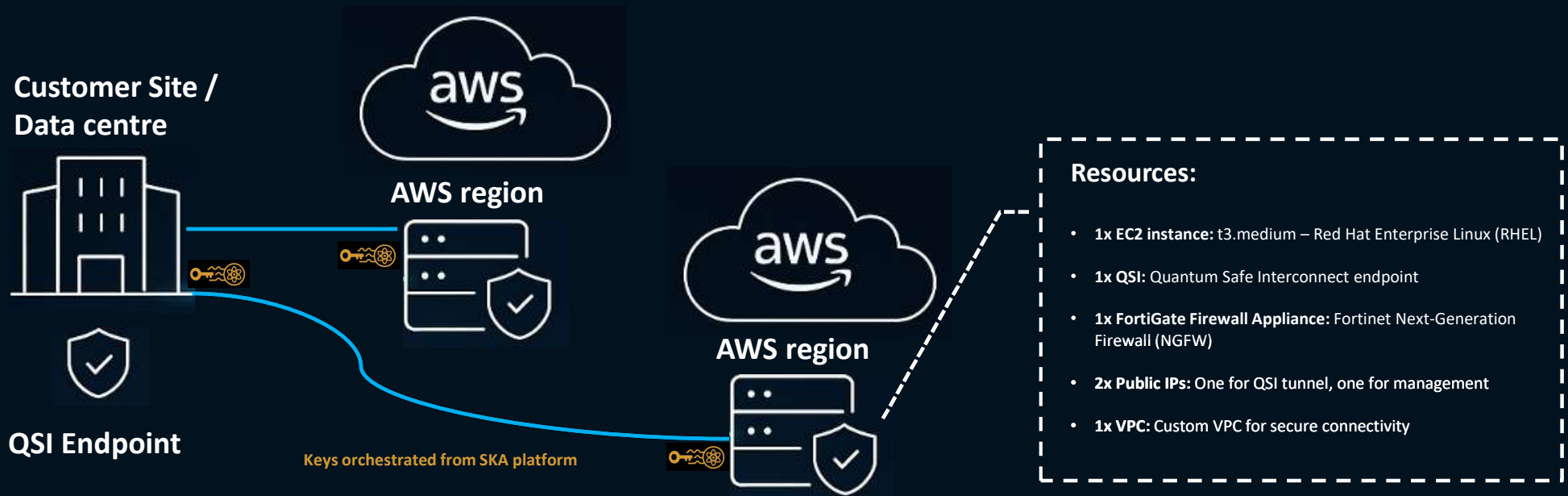
- QSI (Alice) deployed over VM
- QSI (Bob) deployed over uCPE acting as *Key Box Generator*
- Keys provided by QSI are injected into Apollo TM400ENB
- Clear traffic entering TM400ENB network will be encrypted using QSI keys
- Encryption supported per each client interface (10/100GE) independently and line rate up to 400GE



Quantum Safe over Optical – coming soon as the next QSI service option

Quantum Safe to Cloud

Available on AWS



- **Available** on AWS – via Sparkle Channel
- Ordering via AWS Marketplace
- **Quantum-Safe** VPN to Cloud
- Fully managed key orchestration + encrypted transport

Use Cases – Quantum Safe to Cloud



Protecting AI

Post-quantum secure connectivity for sensitive machine learning and AI inference pipelines in transit to AWS



Secure Hybrid Workloads

Quantum-safe VPN tunnels between on-premise edge data centre and AWS VPCs. Ensures post-quantum encryption for mission-critical traffic



Cloud Migration for Sensitive Verticals

Enables secure cloud adoption for finance, healthcare, and public sector.

No infrastructure changes required



Global Site-to-Cloud Interconnect

Carrier-grade performance and quantum-safe transport across regions integrated into Sparkle's NaaS with zero-touch deployment and VNF support

QSI on Equinix

Quantum-safe interconnection for hybrid, multi-cloud and partner ecosystems




Available across 20 Equinix IBX locations with EMS | Europe, Americas and Asia



AMERICAS
Calgary, Chicago, Dallas, Montreal,
Rio de Janeiro, Saint John, São Paulo,
Toronto, Washington D.C.



EMEA
Amsterdam, Barcelona, Dublin, Frankfurt,
Helsinki, London, Madrid, Manchester



APAC
Osaka, Singapore, Tokyo

QSI over Satellite

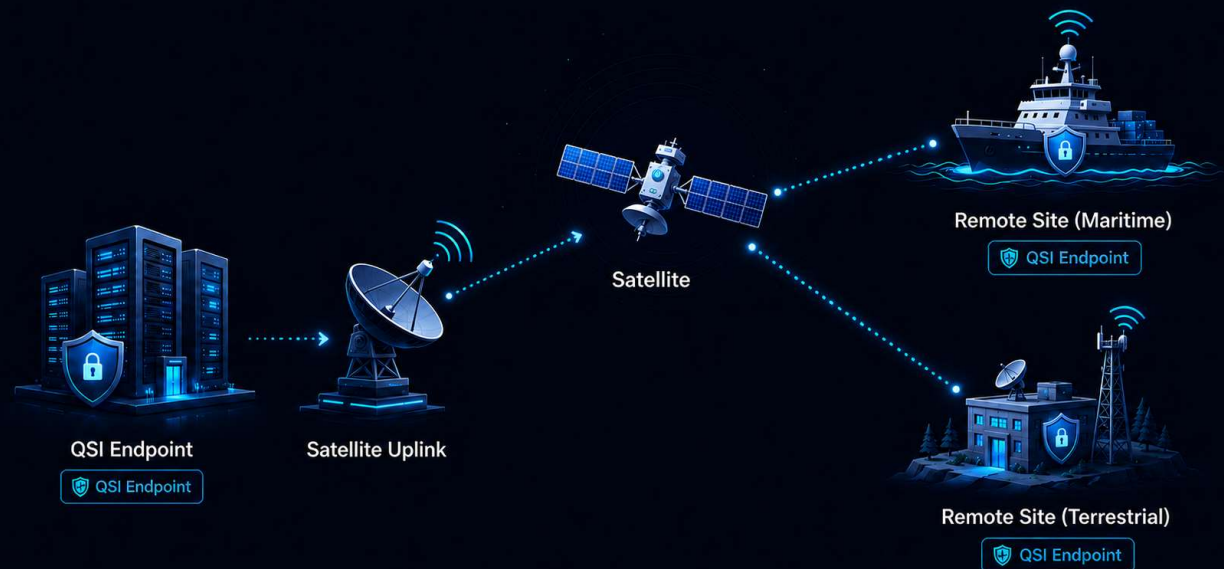
Quantum-safe connectivity for remote, mobile and resilient environments

USE CASE OVERVIEW

- A QSI endpoint protects traffic before satellite transport
- The satellite segment securely extends reach to remote sites
- QSI can connect both maritime and terrestrial endpoints

TYPICAL APPLICATIONS

- Maritime and offshore environments
- Remote terrestrial sites and field locations
- Business continuity and backup access
- Critical communications with distributed endpoints



Lessons learnt from NaaS for Quantum-Safe Connectivity

MARKET ADOPTION LESSONS



Awareness is accelerating

Enterprise discussions are moving from “if quantum-safe” to “**when quantum-safe**”



One crypto strategy across multiple services

Customers prefer a **common security framework** across IP, Ethernet, Cloud and Internet



Compliance drives adoption

PQC readiness is increasingly linked to **regulatory** and **sovereignty** requirements



AI is becoming a catalyst

AI architectures amplify the need for **secure**, **scalable** and **high-performance** connectivity



NAAS & OPERATIONAL LESSONS



Performance cannot be an afterthought

Security controls must coexist with **AI-grade latency** and **throughput** requirements



Automation is mandatory

Quantum-safe services must be provisioned and managed through **APIs** and **NaaS workflows**



Integration is not plug-and-play

Multi-vendor cryptography and network **interoperability** remain key challenges



Crypto-agility is critical

Customers want the ability to **evolve algorithms** without redesigning the network



Availability remains non-negotiable

Security cannot compromise **resiliency** and operational **continuity**



The future of quantum-safe networking is not just stronger cryptography—it is **crypto-agility** delivered through **NaaS**.

THANK YOU!

Antonella Sanguineti
Head of Marketing & Product Management
antonella.sanguineti@tisparkle.com

